Modern Healthcare Jan. 31, 2000
Page 25
Cover Story

The HIPAA lurks: Just when CIOs thought it was safe for business as usual. . .

In the time it took to glimpse the Y2K crisis in their rearview mirrors, healthcare information system executives find themselves confronting a new challenge that may prove even more formidable.
Between this spring and the middle of next year, HCFA will complete the administrative simplification regulations mandated by the Health Insurance Portability and Accountability Act of 1996. The regulations will compel hospitals, health plans and other providers to reconfigure patient records into a uniform electronic format.

HCFA, which issued draft administrative simplification regulations in mid-1998, predicts the healthcare industry will save $1.5 billion during the first five years of HIPAA implementation. Much of this will be achieved by switching from paper claims submission to uniform electronic claims submission. But executives are concerned that the changeover will cost far more than the estimated $8.5 billion spent on Y2K compliance.

"I've heard estimates that this could cost two-and-a-half times what Y2K compliance did," says Bob Blades, chief information officer at Loma Linda (Calif.) University Medical Center. "If that's the case, I'll want to stand behind someone else when I go to my board and ask for an allocation."

John Glaser, vice president and CIO of nine-hospital Partners Healthcare System in Boston, says, "No one knows how much this is all going to cost."

Similar to how they handled Y2K, many hospital CIOs are forming or have already formed exploratory committees to deal with the issue. Consulting firms are gearing up for what they believe will be a sizable book of HIPAA business.

"A couple of healthcare clients we work with have suggested that HIPAA could be bigger than Y2K," says Tim Hicks, executive vice president of marketing at Data Dimensions, a Dallas-based consulting firm that counseled dozens of healthcare clients on Y2K issues.

Moreover, the changes will occur under a glaring public spotlight fueled by concerns that once patient records are transferred to an electronic medium they will be less secure and private.

CIOs and other industry experts have mixed opinions about how daunting the work will be, but all agree it will be far from a cakewalk.

Fighting for delay. Though every healthcare executive interviewed praised the regulations for the way they will modernize recordkeeping, many worry about getting too much of a good thing too soon. Some industry lobbies, such as the American Association of Health Plans and the American Hospital Association, say they will fight to extend HCFA's proposed two-year time frame for HIPAA implementation.

Richard Wade, AHA senior vice president for communications, promises that his organization will lobby for an extension of the deadline. "A three-year timeline is more reasonable," he says. "We have lots of education issues for our members to tackle, and they're going to be spending millions of dollars to comply."

Wade notes that many of his members are still dealing with Y2K issues, and haven't had the time to pore over the 1,000-plus pages of proposed HIPAA regulations. Some state organizations think implementation will take more than three years. For example, officials with the California Healthcare Association say a five-year deadline is reasonable to allow for extensive testing of modified information systems.

CIOs such as Blades and Glaser also say two years is too little time. "Nobody believes it would happen in that time frame, particularly if you took a strong interpretation (of the proposed regulations)," Glaser says. "To have audit trails prepared in two years is just not a practicable proposition."

AAHP spokeswoman Susan Pisano notes that her organization has sensed from its members "the need for more time, but at the moment there's no overwhelming worry. The major concern here is the level of detail that will be presented in the final regulations."

What problem? Yet even as such storm clouds gather on the horizon, HCFA officials and healthcare policymakers on Capitol Hill are all but ignoring them.

The original HIPAA law is now nearly 4 years old-ancient in an era of sound-bite politics. That means few politicians seem to be paying attention to potential industry reaction as the regulations lurch toward completion. Indeed, Congress failed to reach consensus on drafting privacy and security regulations last year, passing the task to HHS and HCFA.

Many House committee aides contacted for this story said they had no knowledge of HIPAA's patient-record provision. When queried about it, one aide to a committee with jurisdiction over health issues replied, "What's that?" Rep. William Thomas (R-Calif.), chairman of the House Ways and Means health subcommittee, declined an interview request.

With HIPAA, legislators aimed to make it easier for providers to switch from traditional paper claims submission and payment to standardized electronic claims submission. In theory, this would simplify the mounds of paperwork associated with many healthcare transactions. Uniformity would also save healthcare organizations billions of dollars per year, because it would eliminate the paper-to-electronic changeover required when an organization that's more electronically savvy does business with one that's less so.

To guarantee HIPAA compliance, providers and health plans will have to jump through these basic hoops:

* Embed 10-digit identification numbers into systems-along with an additional number for each patient, which is likely to be a modified version of the patient's Social Security number. A number is also required for employers, likely their taxpayer identification number. These numbers will act as identifiers during data exchanges.

* Follow uniform information protocols for exchanging patient information that will be established by HHS and HCFA.

* Guarantee the confidentiality of patient records by establishing a multifaceted security process. This applies to conveyors and holders of information.

But HIPAA compliance comes in many shadings, say industry observers.

For example, although data transmissions will be standardized, there are various ways to comply with storage and security regulations. Should a system use something as simple as a password or require a fingerprint or retinal scan to access information? Many hospital and health plan computer systems can handle only 20 lines of code per claim, but HIPAA guidelines say claims can be up to 50 lines long.

"You as a hospital might be able to physically transmit a transaction, but will you have the databases to support it?" asks Shannah Koss, a HIPAA services executive with IBM Global Solutions, which is developing various software applications to address compliance issues.

In other words, should hospitals expend more capital to make as many accommodations as possible? Or should they bypass upgrades in favor of contracting with a third-party information clearinghouse-yet another alternative allowed under the HIPAA regulations.

"This is an opportunity for healthcare institutions to correct the huge inefficiencies of their data transmission process as well as those parts that are prone to error," says Keith MacDonald, manager of the emerging practices group at First Consulting Group in Long Beach, Calif., a healthcare information systems consulting company that has extensively examined HIPAA compliance issues. "This could be the same type of transformation that brought virtually the entire banking industry online a couple of years ago. Those that see this simply as a compliance issue will have missed the boat."

Really big. "Y2K was big, but Y2K was (relatively) easy," says Blades of Loma Linda University Medical Center. "HIPAA is big and wide, and it's more than just information-transmission issues. There's a whole chain of trusts that a multitude of institutions will have to invest in."

Rick Skinner, CIO for 18-hospital Sisters of Providence Health System in Seattle, says HIPAA compliance could be "eerily similar" to Y2K preparation. "Those organizations using software they're not keeping current could wind up with a fairly significant challenge."

A recent newsletter from Cain Brothers investment banking firm summed up the leading concern for the industry, dryly observing that HIPAA "might better be called the Healthcare Information Programmers Annuity Act."

Yet healthcare organizations that are loath to invest in HIPAA compliance sooner rather than later could pay even more. Fines will range from $100 to $25,000 for each violation of

a regulation. Individuals who knowingly violate the patient-confidentiality provisions could face 10 years in prison and a $250,000 fine for each offense. And to make the situation even more onerous, those already costly accreditations from the Joint Commission for the Accreditation of Healthcare Organizations and the National Committee for Quality Assurance could eventually be contingent on HIPAA compliance.

Yet despite their money worries, many CIOs say they are waiting until the regulations are completed before determining what they will have to do and deciding how much of the compliance burden can be shifted to their software vendors.

"It is definitely within the provider perspective that the (information system) vendors will have to fix the problem if they want to stay in business," says IBM's Koss.

Few healthcare executives say they are underestimating the impact of reaching HIPAA compliance, but the palpable sense of an impending deadline that accompanied Y2K appears absent.

"If you blow it on Y2K, the businesses shut down. Here, you get fined," Glaser says. "This is also more focused, where there are no worries about elevators' shutting down or the supply chain's coming to a halt." Moreover, Glaser notes that in following federal mandates, "you can adopt a posture of being victimized by the government" and therefore buy more time.

Only Sisters of Providence's Skinner indicated he's acting immediately: The system's seven hospitals in Oregon are expected to complete policy and procedural work for HIPAA compliance by the end of September and use their work as a template for the rest of the system.

"Maybe I'm cynical, but if you can't change your policy and procedure in two years, you're not committed," he says.

-- Ron Shinkman and Jonathan Gardner